<table>
<tr><th colspan="2">REQUIREMENTS - HIGH Cyber Risk Profile</th></tr>
<tr><th colspan="2">Good Governance</th></tr>
<tr><td colspan="2"><b>L.01</b> Define and assign information security relevant roles and responsibilities.</td></tr>
<tr><td colspan="2"><b>L.02</b> Define and implement a policy that addresses information security risks within supplier relationships.</td></tr>
<tr><td colspan="2"><b>M.01</b> Define and implement a policy that provides for regular, formal information security related reporting.</td></tr>
<tr><th colspan="2">Culture and Awareness</th></tr>
<tr><td colspan="2"><b>L.03</b> Define and implement a policy that ensures all functions have sufficient and appropriately qualified resources to manage the establishment, implementation and maintenance of information security.</td></tr>
<tr><td><b>L.04</b> Define employee (including contractor) responsibilities for information security.</td><td><b>M.02</b> Define and implement a policy to detail specific employee and contractor responsibilities for information security before granting access to sensitive assets.</td></tr>
<tr><td colspan="2"><b>L.05</b> Define and implement a policy to provide employees and contractors with information security training.</td></tr>
<tr><th colspan="2">Risk Management</th></tr>
<tr><td colspan="2"><b>M.03</b> Define and implement a policy that provides for repeatable information security risk assessments.</td></tr>
<tr><th colspan="2">Information</th></tr>
<tr><td><b>L.06</b> Define and implement a policy for ensuring that sensitive information is clearly identified.</td><td><b>M.04</b> Define and implement a policy for storing, accessing, and handling sensitive information securely.</td></tr>
<tr><td colspan="2"><b>M.05</b> Define and implement a policy for data loss prevention.</td></tr>
<tr><td><b>L.07</b> Define and implement a policy to control access to information and information processing facilities.</td><td><b>M.06</b> Ensure that the organisation has identified asset owners and that asset owners control access to their assets.</td></tr>
<tr><th colspan="2">Technology and Services</th></tr>
<tr><td colspan="2"><b>L.08</b> Maintain Cyber Essentials Scheme Plus certification.</td></tr>
<tr><td colspan="2"><b>H.01</b> Maintain patching metrics and assess patching performance against policy.</td></tr>
<tr><td colspan="2"><b>H.02</b> Ensure that wireless connections are authenticated</td></tr>
<tr><td colspan="2"><b>L.09</b> Define and implement a policy to control the exchanging of information via removable media.</td></tr>
<tr><td colspan="2"><b>L.10</b> Define and implement an information security policy, related processes and procedures.</td></tr>
<tr><td colspan="2"><b>L.11</b> Record and maintain the scope and configuration of the information technology estate.</td></tr>
</table>

REQUIREMENTS - HIGH Cyber Risk Profile	
M.07 Define and implement a policy to assess vulnerabilities identified for which there are no countermeasures (e.g. a patch) available, undertake risk assessment and management.	
M.08 Define and implement a policy to monitor network behaviour and review computer security event logs for indications of potential incidents.	**H.03** Deploy network monitoring techniques that complement traditional signature-based detection.
	H.04 Place application firewalls in front of critical servers to verify and validate the traffic going to the server.
	H.05 Deploy network-based Intrusion Detection System (IDS) sensors on ingress and egress points within the network and update regularly with vendor signatures.
L.12 Define and implement a policy to manage the access rights of user accounts.	**M.09** Define and implement a policy to monitor user account usage and to manage changes of access rights.
M.10 Define and implement a policy to control remote access to networks and systems.	
M.11 Define and implement a policy to control the use of authorised software.	**H.06** Define and implement a policy to control installations of and changes to software on any systems on the network.
M.12 Define and implement a policy to control the flow of information through network borders.	**H.07** Control the flow of traffic through network boundaries and police content by looking for attacks and evidence of compromised machines.
M.13 Define and implement a policy to maintain the confidentiality of passwords.	
H.08 Undertake administration access over secure protocols, using multi-factor authentication**.**	
H.09 Design networks incorporating security countermeasures, such as segmentation or zoning.	
H.10 Ensure Data Loss Prevention (DLP) at network egress points to inspect the contents of and, where necessary, block information being transmitted outside of the network boundary.	
Personnel Security	
L.13 Define and implement a policy for verifying an individual's credentials prior to employment.	**M.14** Define and implement a policy for applying security vetting checks to employees.
L.14 Define and implement a process for employees and contractors to report violations of information security policies and procedures without fear of recrimination.	
L.15 Define and implement a disciplinary process to take action against employees who violate information security policies or procedures.	
M.15 Undertake personnel risk assessments for all employees and contractors and ensure those with specific responsibilities for information security have sufficient appropriate qualifications and appropriate levels of appropriate experience.	
M.16 Define and implement a policy to secure organisational assets when individuals cease to be employed by your organisation.	

REQUIREMENTS - HIGH Cyber Risk Profile
Preparing for and Responding to Security Incidents
L.16 Define and implement an incident management policy, which must include detection, resolution and recovery.
H.11 Proactively verify that the security controls are providing the intended level of security.

REQUIREMENTS - HIGH Cyber Risk Profile

Technology and Services

H.01 Maintain patching metrics and assess patching performance against policy.

Evidence Required

Information	**Supplier's Information**	**Further Information**
Patching metrics.	< Metrics identified > <Review Date>	CES Plus requires patching policy. This requirement is to measure performance against this policy. Identify when the performance was last reviewed.

General Guidance

Measure the delay in patching new vulnerabilities.

Alternative countermeasures should be considered if patches are not available.[CSC 4-8]

Evaluate critical patches in a test environment before pushing them into production on enterprise systems. If such patches break critical business applications on test machines, the organization must devise other mitigating controls that block exploitation on systems where the patch cannot be deployed because of its impact on business functionality.[CSC 4-9]

Establish a process to risk-rate vulnerabilities based on the exploitability and potential impact of the vulnerability, and segmented by appropriate groups of assets (example, DMZ servers, internal network servers, desktops, laptops). Apply patches for the riskiest vulnerabilities first. A phased rollout can be used to minimize the impact to the organization. Establish expected patching timelines based on the risk rating level. [CSC 4-10]

REQUIREMENTS - HIGH Cyber Risk Profile		
Technology and Services		
H.02 Ensure that wireless connections are authenticated		
Evidence Required		
Information	**Supplier's Information**	**Further Information**
Authenticate wireless connections	< List Authentication Protocol(s) Used / Not Applicable >	
General Guidance		

Some examples of good practice include:

The Critical Security Controls For Effective Cyber Defense, Version 5.0, CSC 7, Wireless Access Control

“Major thefts of data have been initiated by attackers who have gained wireless access to organizations from outside the physical building, bypassing organizations’ security perimeters by connecting wirelessly to access points inside the organization. Wireless clients accompanying traveling officials are infected on a regular basis through remote exploitation during air travel or in cyber cafes. Such exploited systems are then used as back doors when they are reconnected to the network of a target organization. Still other organizations have reported the discovery of unauthorized wireless access points on their networks, planted and sometimes hidden for unrestricted access to an internal network. Because they do not require direct physical connections, wireless devices are a convenient vector for attackers to maintain long term access into a target environment.”

Ensure that all wireless traffic leverages at least Advanced Encryption Standard (AES) encryption used with at least Wi-

Fi Protected Access 2 (WPA2) protection. [CSC 7-6]

Configure network vulnerability scanning tools to detect wireless access points connected to the wired network. Identified devices should be reconciled against a list of authorized wireless access points. Unauthorized (i.e., rogue) access points should be deactivated. [CSC 7-2]

Disable peer-to-peer wireless network capabilities on wireless clients, unless such functionality meets a documented business need. [CSC 7-8]

Disable wireless peripheral access of devices (such as Bluetooth), unless such access is required for a documented business need.” [CSC 7-9]

Note: If there is a “business need”, this must be risk-assessed and approved

Ensure that wireless networks use authentication protocols such as Extensible Authentication Protocol-Transport Layer Security (EAP/TLS), which provide credential protection and mutual authentication. [CSC 7-7]

For further details visit:

https://www.sans.org/media/critical-security-controls/CSC-5.pdf

BIS 10 Steps to Cyber Security, Network Security

“Wireless devices should only be allowed to connect to trusted wireless networks. All wireless access points should be secured and security scanning tools should have the ability to detect wireless access points.”

For further details visit:

https://www.gov.uk/government/publications/cyber-risk-management-a-board-level-responsibility

<table>
<tr><th colspan="3">REQUIREMENTS - HIGH Cyber Risk Profile</th></tr>
<tr><td colspan="3"><b>Technology and Services</b></td></tr>
<tr><td colspan="3"><b>H.03</b> Deploy network monitoring techniques that complement traditional signature-based detection.</td></tr>
<tr><td colspan="3"><b>Evidence Required</b></td></tr>
<tr><td><b>Information</b></td><td><b>Supplier’s Information</b></td><td><b>Further Information</b></td></tr>
<tr><td><b>Network Monitoring</b></td><td></td><td>Evidence would typically include:
Frequency of review for security event logs
Summary of anomalies identified
Remedial action plan</td></tr>
<tr><td colspan="3"><b>General Guidance</b></td></tr>
<tr><td colspan="3">BIS 10 Steps to Cyber Security, Monitoring
“Monitor all ICT systems: Ensure that the solution monitors all networks and host systems (such as clients and servers) potentially through the use of Network and Host Intrusion Detection Systems (NIDS/HIDS) and Prevention Solutions (NIPS/HIPS), supplemented as required by Wireless Intrusion Detection Systems (WIDS) that work in harmony with the wired IDS. These solutions should provide both signature based capabilities to detect known attacks and heuristic capabilities to detect potentially unknown attacks through new or unusual system behaviour.”
For further details visit:
https://www.gov.uk/government/publications/cyber-risk-management-a-board-level-responsibility</td></tr>
</table>

<table>
<tr><th colspan="3">REQUIREMENTS – HIGH Cyber Risk Profile</th></tr>
<tr><th colspan="3">Technology and Services</th></tr>
<tr><td colspan="3"><b>H.04</b> Place application firewalls in front of critical servers to verify and validate the traffic going to the server.</td></tr>
<tr><th colspan="3">Evidence Required</th></tr>
<tr><th>Information</th><th>Supplier's Information</th><th>Further Information</th></tr>
<tr><td>Firewalls and critical servers.</td><td>Confirmation that critical servers have been identified and firewalls are appropriately placed and configured.</td><td></td></tr>
<tr><th colspan="3">General Guidance</th></tr>
<tr><td colspan="3">Any unauthorized services or traffic should be blocked and an alert generated.
Place application firewalls in front of any critical servers to verify and validate the traffic going to the server. Any unauthorized services or traffic should be blocked and an alert generated. [CSC 11-7]</td></tr>
</table>

REQUIREMENTS - HIGH Cyber Risk Profile		
Technology and Services		
H.05 Deploy network-based Intrusion Detection System (IDS) sensors on ingress and egress points within the network and update regularly with vendor signatures.		
Evidence Required		
Information	**Supplier's Information**	**Further Information**
Network Monitoring	Confirmation that sensors are appropriately placed and configured. (eg via penetration testing).	
General Guidance		

Ensure that automated monitoring tools use behaviour-based anomaly detection to complement traditional signature-based detection. [CSC 5-8]

Use network-based anti-malware tools to identify executables in all network traffic and use techniques other than signature-based detection to identify and filter out malicious content before it arrives at the endpoint. [CSC 5-9]

Configure the built-in firewall session tracking mechanisms included in many commercial firewalls to identify TCP sessions that last an unusually long time. To help identify covert channels exfiltrating data through a firewall. Alert personnel about the source and destination addresses associated with these long sessions. [CSC 13-13]

Configure network boundary devices, including firewalls, network-based IPS, and inbound and outbound proxies, to verbosely log all traffic (both allowed and blocked) arriving at the device. [CSC 14-6]

For all servers, ensure that logs are written to write-only devices or to dedicated logging servers running on separate machines from the hosts generating the event logs, lowering the chance that an attacker can manipulate logs stored locally on compromised machines. [CSC 14-7]

Deploy a SIEM (Security Incident and Event Management) or log analytic tools for log aggregation and consolidation from multiple machines and for log correlation and analysis. Using the SIEM tool, system administrators and security personnel should devise profiles of common events from given systems so that they can tune detection to focus on unusual activity, avoid false positives, more rapidly identify anomalies, and prevent overwhelming analysts with insignificant alerts. [CSC 14-8]

Ensure that the log collection system does not lose events during peak activity, and that the system detects and alerts if event loss occurs (such as when volume exceeds the capacity of a log collection system). This includes ensuring that the log collection system can accommodate intermittent or restricted-bandwidth connectivity through the use of handshaking / flow control. [CSC 14-10]

Enforce detailed audit logging for access to nonpublic data and special authentication for sensitive data. [CSC 15-3]

The IDS should be monitored for alerts. IPS mode should be enabled once normal traffic patterns are understood.

REQUIREMENTS - HIGH Cyber Risk Profile		
Technology and Services		
H.06 Define and implement a policy to control installations of and changes to software on any systems on the network.		
Evidence Required		
Information	**Supplier's Information**	**Further Information**
Software control Policy	<Title> <Issue No> <Issue Date> <Authorised By> <Document Reference> *<Cross-reference> (see Note)*	Identify the policy that defines how software installation and changes are controlled.. *Note: If addressed within a policy for which details are provided elsewhere (against another CSM requirement), simply quote the Policy's Title and cross-reference to the relevant section.*
Software Controls	< Date of Last Scan for Unapproved Software > < Number of Unapproved Software Configurations Detected>	
General Guidance		
See next page.		

General Guidance
Examples of software controls include: Perform regular scanning for unauthorized software and generate alerts when it is discovered on a system. This includes alerting when unrecognized binaries (executable files, DLL's and other libraries, etc.) are found on a system, even inside of compressed archives. This includes checking for unrecognized or altered versions of software by comparing file hash values (attackers often utilize altered versions of known software to perpetrate attacks, and file hash comparisons will reveal the compromised software components). Deploy software inventory tools throughout the organization covering each of the operating system types in use, including servers, workstations, and laptops. The software inventory system should track the version of the underlying operating system as well as the applications installed on it. Furthermore, the tool should record not only the type of software installed on each system, but also its version number and patch level. [CSC 2-4] Utilize file integrity checking tools to ensure that critical system files (including sensitive system and application executables, libraries, and configurations) have not been altered. All alterations to such files should be automatically reported security personnel. The reporting system should have the ability to account for routine and expected changes, highlighting unusual or unexpected alterations. [CSC 3-8] Implement and test an automated configuration monitoring system that measures all secure configuration elements that can be measured through remote testing and alerts when unauthorized changes occur. Use features such as those included with tools compliant with Security Content Automation Protocol (SCAP). This includes detecting new listening ports, new administrative users, changes to group and local policy objects, (where applicable), and new services running on a system. [CSC 3-9] Deploy system configuration management tools that will automatically enforce and re-deploy configuration settings to systems at regularly scheduled intervals. Such as Active Directory Group Policy Objects for Microsoft Windows systems or Puppet for UNIX systems. They should be capable of triggering redeployment of configuration settings on a scheduled, manual, or event-driven basis.[CSC 3-10] Use automated tools to verify standard device configurations and detect changes. All alterations to such files should be automatically reported to security personnel. [CSC 10-3]

REQUIREMENTS - HIGH Cyber Risk Profile		
Technology and Services		
H.07 Control the flow of traffic through network boundaries and police content by looking for attacks and evidence of compromised machines.		
Evidence Required		
Information	**Supplier's Information**	**Further Information**
Unauthorised VPN Connections	< Date of last scan for unauthorised VPN connections > Confirmation of removal of connections and that the vulnerability has been addressed.	
General Guidance		

Boundary control could include:

Periodically scan for back-channel connections to the Internet that bypass the DMZ, including unauthorized VPN connections and dual-homed hosts connected to the enterprise network and to other networks via wireless, dial-up modems, or other mechanisms.[CSC 13-9]

Only allow DMZ systems to communicate with private network systems via application proxies or application-aware firewalls over approved channels. To minimize the impact of an attacker pivoting between compromised systems.[CSC 13-12] [CSC 17-9]

Monitor all traffic leaving the organization and detect any unauthorized use of encryption. Attackers often use an encrypted channel to bypass network security devices. Therefore it is essential that organizations be able to detect rogue connections, terminate the connection, and remediate the infected system. [CSC 17-12]

Where applicable, implement Hardware Security Modules (HSMs) for protection of private keys (e.g., for sub CAs) or Key Encryption Keys.[CSC 17-15]

Policing options include:

CSC 13-4] Deploy network-based IDS sensors on Internet and extranet DMZ systems and networks that look for unusual attack mechanisms and detect compromise of these systems. These network-based IDS sensors may detect attacks through the use of signatures, network behavior analysis, or other mechanisms to analyze traffic

[CSC 13-5] Network-based IPS devices should be deployed to complement IDS by blocking known bad signature or behavior of attacks. Network-based IPS devices should be deployed to complement IDS by blocking known bad signature or behavior of attacks. As attacks become automated, methods such as IDS typically delay the amount of time it takes for someone to react to an attack. A properly configured network-based IPS can provide automation to block bad traffic. When evaluating network-based IPS products, include those using techniques other than signature-based detection (such as virtual machine or sandbox-based approaches) for consideration.

REQUIREMENTS - HIGH Cyber Risk Profile		
Technology and Services		
H.08 Undertake administration access over secure protocols, using multi-factor authentication**.**		
Evidence Required		
Information	**Supplier's Information**	**Further Information**
Secure Administration	< Number of factors used for authentication of administrators >	All administrative access is conducted over secure protocols, using multi- factor authentication
General Guidance		
Controls on administrative access could include: Manage the network infrastructure across network connections that are separated from the business use of that network. Use separate VLANs or, preferably, entirely different physical connectivity for management sessions for network devices. [CSC 10-6] Use multifactor authentication for all administrative access, including domain administrative access. Multi-factor authentication can include a variety of techniques, to include the use of smart cards with certificates, One Time Password (OTP) tokens, and biometrics. [CSC 12-12] When using certificates to enable multi-factor certificate-based authentication, ensure that the private keys are protected using strong passwords or are stored in trusted, secure hardware tokens. [CSC 12-13] Administrators should use different accounts for performing admin roles and normal user roles. Consider the use of password vaulting technology. [CSC 12-14]		

REQUIREMENTS - HIGH Cyber Risk Profile		
Technology and Services		
H.09 Design networks incorporating security countermeasures, such as segmentation or zoning.		
Evidence Required		
Information	**Supplier's Information**	**Further Information**
Secure Network Architecture	< Yes, / Not Applicable >	Confirmation that networks are designed to incorporate security countermeasures, such as segmentation or zoning. Network diagrams should demonstrate this..
General Guidance		
Countermeasures could include: Segment the network based on the trust levels of the information stored on the servers. Whenever information flows over a network with a lower trust level, the information should be encrypted. [CSC 15-4] Deploy domain name systems (DNS) in a hierarchical, structured fashion, with all internal network client machines configured to send requests to intranet DNS servers, not to DNS servers located on the Internet. These internal DNS servers should be configured to forward requests they cannot resolve to DNS servers located on a protected DMZ. These DMZ servers, in turn, should be the only DNS servers allowed to send requests to the Internet. [CSC 19-3] All servers and services should be behind a firewall (virtual or physical) and only services required by the end user should be made available. All ports and protocols not required should be disabled.		

REQUIREMENTS - HIGH Cyber Risk Profile		
Technology and Services		
H.10 Ensure Data Loss Prevention (DLP) at network egress points to inspect the contents of and, where necessary, block information being transmitted outside of the network boundary.		
Evidence Required		
Information	**Supplier's Information**	**Further Information**
Data Loss Prevention	< Yes, / Not Applicable >	Confirmation that a Data Loss Prevention tool is deployed (correctly placed and configured) on network egress points (which inspects the contents of and, where necessary, blocks information being transmitted outside of the network boundary).
General Guidance		

DLP techniques include:

Use host-based data loss prevention (DLP) to enforce ACLs even when data is copied off a server. In most organizations, access to the data is controlled by ACLs that are implemented on the server. Once the data have been copied to a desktop system, the ACLs are no longer enforced and the users can send the data to whomever they want. [CSC 15-5]

Require multi-factor authentication for accounts that have access to sensitive data or systems. Multi-factor authentication can be achieved using Smart cards with certificates, One Time Password (OTP) tokens, or biometrics. [CSC 16-14]

Deploy an automated tool on network perimeters that monitors for certain sensitive information (i.e., personally identifiable information), keywords, and other document characteristics to discover unauthorized attempts to exfiltrate data across network boundaries and block such transfers while alerting information security personnel. [CSC 17-5]

Note: PII should be protected at all levels.

Ensure users apply a classification to data and email based on the sensitivity.

CSC 13-4] Deploy network-based IDS sensors on Internet and extranet DMZ systems and networks that look for unusual attack mechanisms and detect compromise of these systems. These network-based IDS sensors may detect attacks through the use of signatures, network behavior analysis, or other mechanisms to analyze traffic

[CSC 13-5] Network-based IPS devices should be deployed to complement IDS by blocking known bad signature or behavior of attacks. Network-based IPS devices should be deployed to complement IDS by blocking known bad signature or behavior of attacks. As attacks become automated, methods such as IDS typically delay the amount of time it takes for someone to react to an attack. A properly configured network-based IPS can provide automation to block bad traffic. When evaluating network-based IPS products, include those using techniques other than signature-based detection (such as virtual machine or sandbox-based approaches) for consideration.

REQUIREMENTS - HIGH Cyber Risk Profile		
Preparing for and Responding to Security Incidents		
H.11 Proactively verify that the security controls are providing the intended level of security.		
Evidence Required		
Information	**Supplier's Information**	**Further Information**
Tests and Exercises	< Date of last Penetration Test > < Date of next planned Penetration Test > < Date of last Red Team Exercise >	

General Guidance

BIS 10 Steps to Cyber Security, Network Security

"Conduct regular penetration tests of the network infrastructure and undertake simulated cyber attack exercises to ensure that all security controls have been implemented correctly and are providing the necessary level of security."

For further details visit:

https://www.gov.uk/government/publications/cyber-risk-management-a-board-level-responsibility

Perform periodic Red Team exercises to test organizational readiness to identify and stop attacks or to respond quickly and effectively. [CSC 20-3]

Include tests for the presence of unprotected system information and artifacts that would be useful to attackers, including network diagrams, configuration files, older penetration test reports, e-mails or documents containing passwords or other information critical to system operation. [CSC 20-4]

Create a test bed that mimics a production environment for specific penetration tests and Red Team attacks against elements that are not typically tested in production, such as attacks against supervisory control and data acquisition and other control systems. [CSC 20-8]

Details of companies which can assist with testing and incident recovery can be found at:

http://www.cesg.gov.uk/servicecatalogue/service_assurance/CHECK/Pages/CHECK.aspx

http://www.cesg.gov.uk/servicecatalogue/service_assurance/CIR/Pages/Finding-a-Service-Provider.aspx